METHOD AND APPARATUS FOR FACILITATING EFFICIENT AUTHENTICATED ENCRYPTION

ABSTRACT

A shared-key encryption scheme that uses identically keyed block-cipher calls, low additional overhead, supports the encryption of arbitrary-length strings, produces a minimal-length-ciphertext, and is fully parallelizable. In one embodiment, "OCB", a key shared between communicating parties is mapped to a key variant using the block cipher. The key variant is mapped into a sequence of basis offsets using shifts and conditional xors. To encrypt a message using a nonce, a nonce-dependent base offset is formed, and then a sequence of offsets is constructed by starting with the base offset and then xoring, for each offset, an appropriate basis offset. The message is partitioned into message blocks of the same length as the block length of the block cipher, along with a message fragment that may be shorter. Each message block is combined with a corresponding offset, enciphered, and then combined again with the offset, yielding a ciphertext block. The message fragment is xored with an appropriately computed pad to give a ciphertext fragment. A checksum is formed using the message blocks, the message fragment, and the pad. The checksum is combined with an offset and enciphered to yield a tag. The encrypted message includes the ciphertext blocks, the ciphertext fragment, and the tag.